

THIS DOCUMENT IS A CONTINUATION SHEET OF BLOCK 13 OF DD FORM 254,  
DATED 4 AUGUST 1997, PAGE 3 OF 8 PAGES

General: The COR must be notified and approve the receipt and/or generation of all classified information under this contract.

Prospective contractors shall have SECRET clearances in order to review the statement of work and other supporting documents for the purpose of making bids.

The selected contractor shall have personnel cleared at the TOP SECRET/SCI level for the purpose of performing the work. Prospective bidders must have people at the SECRET clearance level to evaluate contract materials pertinent to bid preparation.

Access restrictions are required for entry to the SVTS Design, Engineering and Integration (DE&I) facility. Although the SVTS hardware is unclassified, the hardware configuration and the information presented on the consoles reveal sensitive, classified (SECRET) capabilities of the SVTS. The DISA project office will validate all requests for access.

Contractor employees who will require physical access to the various sites to conduct site surveys, installations, testing, follow-on maintenance, etc., must be processed under the provisions of DOD Directive 5210.55. "Classified Visit Requests" by contractors shall be forwarded to the COR for approval and need-to-know certification before being sent to the facility to be visited.

Re Item 10a.

The contractor is authorized to receive Government furnished cryptographic equipment. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. Further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior approval of the contracting activity.

Re Item 10e(1).

1. The contract requires access to Sensitive Compartmented Information (SCI).

a. The Director, Defense Intelligence Agency (DIA) and Director, Defense Information Systems Agency (DISA), as the executive agents for DIA, has exclusive security responsibility for SCI information released to the contractor or developed under this contract.

b. Contractor generated or Government furnished material may not be provided to the Defense Technical Information Center (DTIC). Contract generated technical reports will bear the statement **“Not Releaseable to the Defense Technical Information Center per DoD Instruction 5230.24.”**

c. All contractor personnel requiring access to SCI information must: be U.S. citizens; have been granted a final Top Secret security clearance by the Government; have been approved as meeting DCID 1/14 criteria by a government cognizant authority; and have been indoctrinated for the applicable compartments of SCI access prior to being given access to such information released or generated under this contract. Immigrant aliens, interim cleared personnel or personnel holding a contractor granted CONFIDENTIAL clearance are not eligible for access to classified information released or generated under this contract without the express permission of the DISA (SSO) and the Director, DIA.

d. Classified material released or generated under this contract is not releasable to foreign nationals without the express permission of the DISA SSO and Director, DIA.

e. Recipients of SCI information under this contract may not release information to subcontractors without permission of DISA SSO.

f. STU-III terminals installed at the contractor's facilities shall be supported by a COMSEC account (of the contractor of DISA). STU-IIIs in SCI Facilities (SCIFs) require Class VI Cryptographic Ignition Key (CIK).

g. The contractor and COR will revalidate all SCI billets under this contract with the DISA Security Operations Division (D162) annually or when a revised DD Form 254 is issued, whichever is sooner.

THIS DOCUMENT IS A CONTINUATION SHEET OF BLOCK 13 OF DD FORM 254,  
DATED 4 AUGUST 1997, PAGE 5 OF 8 PAGES

Re Item 10e(1).

Upon expiration of the contract the contractor shall request disposition instructions for all classified and unclassified project material. The contractor may be directed to properly destroy the material or return it.

Contractor requests to retain classified material after expiration shall be directed to the Contracting Officer (CO) and shall clearly indicate the justification for retention and the period of time retention is necessary.

If classified or unclassified project material is to be retained by the contractor, every effort should be taken to transfer it to a follow-on contract or similar effort, if applicable. This must be done however, with CO(s) approval.

Unless written authorization by the CO to retain specific material for a specific period of time is received, the material will be returned or destroyed as instructed.

Any exception to security policy shall be referred to the CSA/SSO DISA for coordination with the appropriate agencies and the Contracting Officer.

Re Item 10j.

For Official Use Only information provided under this contract shall be safeguarded as specified in DOD Regulation 5400.7, DOD Freedom of Information Act Program.

Re Item 11c.

Classified documents generated under this contract will be marked in accordance with the Industrial Security Manual DOD 5220.22-M and with the guidance provided in the SVTS Network Security Manual (U), May 1997.

The contractor shall be authorized to designate a responsible employee as a courier for handling TOP SECRET materials.

THIS DOCUMENT IS A CONTINUATION SHEET OF BLOCK 13 OF DD FORM 254,  
DATED 4 AUGUST 1997, PAGE 6 OF 8 PAGES

For the purpose of classified Automated Information Systems (AIS) processing, it has been determined that it is in the best interest of the Government to assume a common need-to-know exists between information developed under the predecessors, successors, and derivatives of this contract. This determination allows the commingling of classified information on AIS storage media and the simultaneous processing of information. The following precautions must be taken:

- a. Classified storage media is protected and controlled to the standards required by the highest category of information contained in the media.
- b. Procedures exist to ensure that derivative classification markings are properly assigned to any printed document produced for AIS, i.e., files that can be traced to the original contract.
- c. Processing of SCI/SAP must be accomplished on equipment accredited in accordance with DIAM 50-5, Vol II and DIAM 50-4.

The contractor shall prepare an ADP/Standard Practice and Procedures for their ADP operations and the system will require approval of the CSO/CSA in accordance with the NISPOM.

Re Item 11d.

There will be a Government-leased facility called the Design, Engineering and Integration Facility or DE&I facility in which the contractor will do software testing and development work and hardware integration and testing. In this facility the contractor will maintain three equipment racks each 4'X4' which contain electronic encryption devices. These devices are unclassified when not keyed but they are cryptographic controlled items. The equipment will assume the classification of the key after the key has been loaded. The key is classified CONFIDENTIAL. The contractor will need five metal safes to store classified documents and software classified at the SECRET level. CONFIDENTIAL cryptographic keys will also be stored.

THIS DOCUMENT IS A CONTINUATION SHEET OF BLOCK 13 OF DD FORM 254,  
DATED 4 AUGUST 1997, PAGE 7 OF 8 PAGES

Re Item 11e.

Contract is for engineering services and for maintenance services.

- For engineering services. Classification markings on the material to be furnished will provide the classification guidance necessary for performance of this contract.

- For equipment maintenance services. The maintenance portion of this contract is for equipment maintenance services on equipments which process classified information. Actual knowledge of, generation, or production of classified information is not required for performance of the contract. Cleared personnel are required to perform this service because access to classified information can not be precluded by escorting personnel. Any classification guidance needed will be provided by the using activity.

Re Item 11i.

The contractor shall prepare an ADP/Standard Practice and Procedures for his ADP operations. These procedures must be approved by the CSO in accordance with the NISPOM.

The contractor shall not process classified information by electrical means prior to a DISA TEMPEST evaluation of the equipment/systems and facility, and written DISA certification that the facility meets DISA TEMPEST criteria. In order to expedite the DISA TEMPEST evaluation, the contractor shall provide a list of equipment to the DISA Certified Tempest Technical Authority, to include model number, that is associated with processing classified information. In addition, the estimated percentage of classified information processed, cable/conduit runs, a floor plan layout that depicts placement of equipment and telephones will be furnished. The drawings(s) are to show dimensions of rooms, physical relation to other rooms, equipment distances for walls or uncontrolled areas, and physical security being afforded the equipment both during processing and after hours.

The above TEMPEST evaluation and DISA approval will not be required if previous DISA approval can be furnished and is no more than two years old. The existing approval must be for processing information of the same or higher level security classification and for the same facility and items of equipment.

The operational equipment at the SVTS sites shall be capable of processing TOP SECRET/SCI information, however the highest level of information processed at the contractor facility shall be the SVTS software which is classified SECRET.

THIS DOCUMENT IS A CONTINUATION SHEET OF BLOCK 13 OF DD FORM 254,  
DATED 4 AUGUST 1997, PAGE 8 OF 8 PAGES

Re Item 11l.

The contractor shall maintain a Standard Practice Procedures (SPP) for both the facility and AIS that have been approved by the DISA SSO to implement the security requirements for this contract. The procedures shall establish guidelines and implementing instructions on how the contractor shall protect the security of the project during all phases of the effort. These procedures shall be based on the NISPOM as supplemented by Special Access Program manuals, directives or regulations and shall explain all aspects of project security as they apply to the specific contractor facility. The SPP shall be kept current and updated as necessary to meet changing project requirements. Prior to implementation, the SPP shall be approved by the DISA SSO. The SPP shall be classified according to content based on the DOD classification guide provided by the SSO as part of this contract.

Upon expiration of the contract, all classified and unclassified project material shall be returned within 10 days to the COR unless written authorization to retain or destroy the material is granted. Contractor requests to retain government material after expiration shall be directed to the Contracting Officer and shall clearly indicate the justification of retention and the period of time retention is necessary.

Re Item 14.

1. SVTS Network Security Manual, May 1997
2. DoD Regulation 5400.7, DoD Freedom of Information Act Program
3. NSA Manual 90-2, COMSEC Material Control Manual
4. Defense Intelligence Agency Manual 50-4, Security of Compartmented Computer Operations
5. Defense Intelligence Agency Manual 50-5, Volumes I & II, Sensitive Compartmented Information (SCI) Contractor Administrative Security
6. Director, Central Intelligence Directive 1/21, Physical Security Standards for SCI